Digitaliserings-
styrelsen

Til høringsparterne

04. november 2024

Høring om OIOSAML 4

Digitaliseringsstyrelsen sender hermed den kommende version 4 af OIOSAML profilen i offentlig høring.

Baggrunden for opdateringen af profilen er ønsket om at kunne håndtere digitale identiteter fra andre EU-lande, idet en række offentlige tjenesteudbydere er underlagt krav om at kunne modtage EU-identiteter i medfør af eIDAS- og SDG-forordningerne. Med henblik på at lette byrderne for tjenesteudbydere, der skal modtage forskellige typer af identiteter fra en broker, har Digitaliseringsstyrelsen valgt at indbygge den nødvendige understøttelse heraf direkte i den nye version 4 af profilen.

I dag har en række offentlige tjenesteudbydere foretaget en integration med OIOSAML 3 snitfladen til NemLog-in for at modtage danske identiteter, samtidig med at de har en separat integration til Digitaliseringsstyrelsens eID-gateway baseret på en anden variant af SAML protokollen med henblik på at kunne modtage EU-identiteter. Med OIOSAML 4 vil det blive muligt at modtage mange forskellige typer autentificerede identiteter via én og samme snitflade, hvilket kan strømline og lette tjenesteudbydernes implementering.

Det er Digitaliseringsstyrelsens plan at tilbyde OIOSAML 4 snitfladen via NemLog-in brokeren i forbindelse med en kommende integration mellem den nuværende eID-gateway og NemLog-in. Digitaliseringsstyrelsen har i anden sammenhæng kommunikeret til tjenesteudbydere tilsluttet den nuværende eID-gateway om den kommende integration på Digitaliseringsstyrelsens hjemmeside (https://digst.dk/it-loesninger/eid-og-single-digital-gateway/vejledninger-til-myndigheder-om-sdg-forordningen/)

Herved bliver det muligt for tjenesteudbydere tilsluttet NemLog-in at modtage både danske identiteter og EU-identiteter via én og samme OIOSAML-integration, og tjenesteudbyderes omkostninger til overholdelse af eIDAS- og SDG forordningerne begrænses herved.

Gradvis indfasning

Digitaliseringsstyrelsen planlægger at indføre OIOSAML 4 profilen til tjenesteudbydere og sub-brokere uden faste deadlines for migrering væk fra OIOSAML 3. Migreringen vil således være drevet af tjenesteudbyderes egne ønsker og behov for at anvende de nye muligheder i OIOSAML 4. Ligeledes er det planen, at den offentlige NemLog-in broker parallelt vil understøtte OIOSAML 3 og 4 endepunkter, således at ingen tjenesteudbydere på kort sigt tvinges til at opgradere sin integration.

Vigtigste ændringer og tilføjelser i OIOSAML 4

Generelt er ændringerne i profilen søgt indført ved udvidelser frem for ændringer af eksisterende mekanismer, så overgangen kan blive så smidig som mulig.

De vigtigste tilføjelser i profilen er oplistet her:

1. Der er indført mekanismer til eksplicit navngivning og håndtering af attributprofiler, hvilket gør det muligt at deklarere (metadata), efterspørge (AuthnRequest) og modtage (Assertion) forskellige typer identiteter med forskelligt attributsæt.

2. Der er defineret en række nye attributprofiler for eIDAS-identiteter, herunder 'person', 'legal person' og 'professional', og der er ligeledes indført flere eksplicitte DK-attributprofiler herunder til håndtering af identiteter uden CPR-nummer eller anonymiserede identiteter. Attributprofilernes eksplicitte navngivning giver større sikkerhed for identitetens type og dermed det forventelige attributsæt.

3. For hver attributprofil er det tydeligere markeret, om den enkelte attribut er obligatorisk, om den skal være understøttet af Identity Providers (hvis efterspurgt), eller om den er frivillig at tilbyde. Skelnen mellem obligatorisk, understøttet og frivillig giver større klarhed og forudsigelighed for tjenesteudbyderne og deres lokale forretningslogik.

4. For eIDAS-attributprofilerne er medtaget de attributter, der er specificeret i eIDAS SAML-profilerne fra EU-kommissionen. Det er disse attributter, der kan forventes leveret af eID-gateways fra de øvrige EU-lande.

5. OIOSAML profilen håndterer sikringsniveauer (Levels of Assurance, LoA) både under eIDAS- og NSIS-rammeværk, samt definerer en generisk LoA-attribut for de tjenesteudbydere, der ikke ønsker at skelne mellem sikringsniveauer under NSIS og eIDAS.

6. Det er muligt at angive via en attribut (provider), hvilken up-stream IdP som har foretaget brugerautentifikationen.

7. Der er indført en ny attribut (isRobot), som gør det muligt at deklarere, at identiteten er en robotidentitet. Denne er tiltænkt fremtidige scenarier, hvor softwarerobotter kan få egne eksplicitte identiteter til at autentificere sig med over for en broker.

8. Der er indført en ny attribut (allowQualifiedSigning), som gør det muligt at deklarere, om identiteten er registreret på en måde, der opfylder kravene til kvalificeret signering i henhold til eIDAS-forordningen. Denne kan understøtte scenarier, hvor en autentifikation er grundlaget for dannelse af en kvalificeret signatur.

9. Det er endvidere blevet muligt at angive koblingsstyrken for CPR-numre (attributten CPR IAL). Denne er tiltænkt scenarier, hvor en udenlandsk (eIDAS)identitet formidles med ét sikringsniveau fra en udenlandsk eID-gateway, mens dansk CPR efterfølgende tilføjes i det danske brokerlag på baggrund af en proces, der ikke nødvendigvis har samme sikringsniveau og proveniens som den oprindelige identitet.

Supplerende forhold

OpenID Connect-profiler opdateres efterfølgende

Digitaliseringsstyrelsen har udover OIOSAML profilerne også specificeret danske profiler af OpenID Connect (OIDC) på Digitaliseringsstyrelsen hjemmeside (https://digst.dk/it-loesninger/standarder/openid-connect-profiler/).

Efter at OIOSAML 4 løsningen er endelig, vil der på et senere tidspunkt blive gennemført en tilsvarende opdatering af disse profiler, så de bliver funktionelt ækvivalente.

eID gateway er stadig en mulighed

Det vil fremover fortsat være en mulighed at integrere direkte til den nuværende eID gateway for tjenesteudbydere, der har brug for at kunne modtage EU identiteter. Dette kan bl.a. hjælpe tjenesteudbydere, der har et presserende behov, og ikke kan vente på, at OIOSAML 4 snitfladen bliver tilgængelig i NemLog-in. Oplysninger om dette findes

på Digitaliseringstyrelsens hjemmeside (https://digst.dk/it-loesninger/eid-og-single-digital-gateway/)

Digitale identitetstegnebøger

De nye eIDAS-attributprofiler i OIOSAML 4 er baseret på eIDAS SAML profilerne, der er udviklet til den første udgave af eIDAS-forordningen, som understøtter autentifikation med udenlandske eID'er der er anmeldt til EU-kommissionen og har gennemgået et såkaldt peer review med henblik på at fastlægge deres efterlevelse af kravene. I forbindelse med at den nye udgave af eIDAS-forordningen (vedtaget i 2024) på sigt udmønter digitale identitetstegnebøger ('EUDI Wallets'), kan der forekomme mindre justeringer i OIOSAML attributprofilerne. Det forventes dog, at snitfladen i meget høj grad kan holdes stabil, så det også bliver muligt at modtage autentifikationer med identitetstegnebøger via OIOSAML 4 snitfladen. Det er en klar målsætning, at det bliver så transparent som muligt for en dansk tjenesteudbyder, om en bruger har autentificeret sig med et eID eller en identitetstegnebog, så tjenesteudbyderen ikke behøver at foretage specialhåndtering i sin applikation. Dette understøttes af, at attributsættene i de foreløbige specifikationer for identitetstegnebøgerne har en meget høj grad af kongruens med eIDAS SAML attributprofilerne.

Videre proces

Høringen er sendt til de myndigheder og organisationer, der fremgår af vedlagte høringsliste.

Den reviderede OIOSAML 4 profil samt dette høringsbrev offentliggøres desuden på www.hoeringsportalen.dk/

På baggrund af modtagne høringssvar udarbejdes et høringsnotat, som offentliggøres på Høringsportalen efter høringsfristens udløb sammen med eventuelle yderligere tilretninger til OIOSAML 4 profilen.

Den endelige OIOSAML 4 profil forventes publiceret i januar 2025.

Frist og kontaktmuligheder

Digitaliseringsstyrelsen skal anmode om at modtage eventuelle bemærkninger senest onsdag den 04.12 2024 kl. 12.00.

Eventuelle bemærkningerne kan sendes til: nemlogin@digst.dk

Vedlagt høringsliste med oversigt over hørte myndigheder og organisationer.